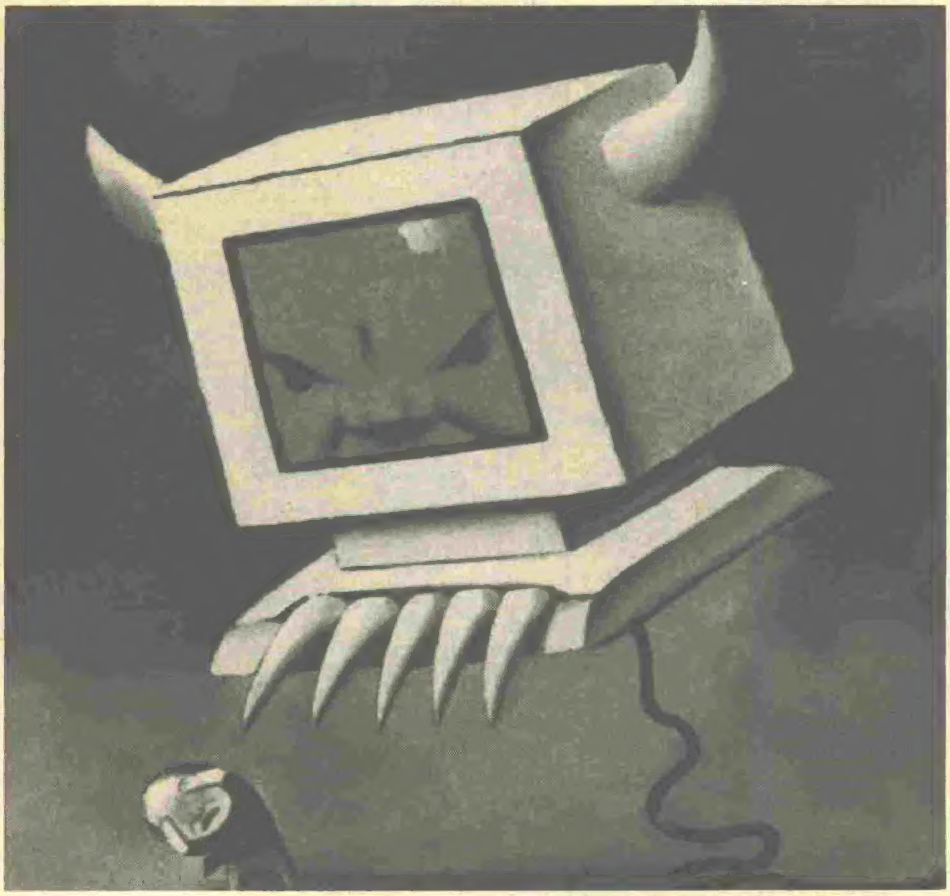
กนิษฐา ปัญญาภรณ์

Boza

ไวรัสตัวแรกบนวินโดวส์ 95



ลางร้ายสำหรับผู้ใช้วินโดวส์ 95 เมื่อ Boza ไวรัสตัวแรก ถือกำเนิดขึ้นมา

Boza ไวรัสขนานแท้ตัวแรกของโลกที่แพร่ระบาดบนวินโดวส์ 95 ถือกำเนิดขึ้นเป็นครั้งแรกในประเทศออสเตรเลีย สร้างความหวั่นไหวให้กับผู้ใช้งานวินโดวส์ 95 กันอย่างทั่วถึง ถูกเขียนขึ้นโดยใช้โค้ดคำสั่งแบบ 32 บิต เพื่อมุ่งจู่โจมไฟล์ .EXE เมื่อมีโอกาส ถึงแม้ว่าจะยังแพร่กระจายไม่ได้มากเท่าที่ควร แต่ก็นับได้ว่าเป็นต้นกำเนิดของไวรัสบนวินโดวส์ 95 ทีเดียว

นับจากที่ไมโครซอฟต์ได้ฤกษ์คลอดวินโดวส์ 95 ออกมาเมื่อวันที่ 24 สิงหาคม 2538 ก็เกือบจะพร้อม ๆ กันกับแอพพลิเคชันซอฟต์แวร์บนวินโดวส์ 95 จากสารพัดค่ายที่คลอดตามกันมาไม่หยุดหย่อน ทำให้ผู้ที่กำลังให้ความสนใจในวินโดวส์ 95 ทั้งหลายเริ่มมีคำถามซ้ำ ๆ กันเกิดขึ้น ...DOS...Windows... ...DOS...Virus... ...Windows...Virus...??? ในเมื่อบนดอสยังมีไวรัส แล้ววินโดวส์ที่บูมกันสุด ๆ ไปเลยในปัจจุบันนี้ล่ะ เป็นไปได้มั้ยว่าอาจจะมีไวรัสเกิดขึ้นมาบ้าง เหล่านี้ล้วนเป็นเพียงคำถามที่ยังหาคำตอบไม่ได้ จวบจนกระทั่ง 1 เดือนถัดมา (ปลายเดือนกันยายน) ก็เกิดมีไวรัสพันธุ์ใหม่ออกมาแพร่ระบาด แปลกกว่าทุกครั้งก็ตรงที่ ไวรัสชนิดนี้ไม่ได้ติดที่บูตเซคเตอร์หรือมาสเตอร์บูตเรคอร์ด ไม่ได้ติดที่ไฟล์นามสกุล .EXE, .COM, .SYS หรือแม้แต่ OVL แต่กลับติดที่ไฟล์เอกสารของไมโครซอฟต์เวิร์ดตั้งแต่เวอร์ชัน 6.0 ขึ้นไป ทั้งบนวินโดวส์ 3.1 และวินโดวส์ 95 รวมทั้งบนเครื่องแมคอินทอชก็ไม่เว้น ไวรัสนี้ถูกขนานนามว่า Winword.Concept, WW6Macro หรือ Prank Macro เกิดเป็นตระกูลของไวรัสประเภทใหม่ที่เรียกว่า WinWord Virus

ถึงแม้เจ้า WinWord Virus ตัวแรกนี้จะไม่มีพิษสงอะไรมากมายนัก แต่ก็เล่นเอาผู้ใช้งานบนวินโดวส์ทั้งหลายเริ่มมีอาการร้อน ๆ หนาว ๆ ไปตาม ๆ กัน เพราะนั่นเหมือนเป็นลางร้ายที่บ่งบอกว่า โอกาสที่จะเกิดไวรัสซึ่งติดไฟล์บนวินโดวส์จริง ๆ โดยเฉพาะวินโดวส์ 95 นั้นมีมากเหลือเกิน

และหลังจากนั้นก็เริ่มมี WinWord Virus ตัวอื่น ๆ ทยอยกันออกมาเรื่อย ๆ ไม่ว่าจะเป็น WinWord.DMV-Demo (หรือ DMV), Nuclear Virus (หรือ PH33R) และ Hot (หรือ QLHot) ซึ่งเติบโตขึ้นทุก ๆ วัน จากทารกน้อยก็เริ่มเติบใหญ่ขึ้นเรื่อย ๆ พอ ๆ กับความร้ายกาจที่มีมากขึ้นเช่นกัน

มาถึงเดือนมกราคม 2539 ไวรัสบนวินโดวส์ 95 ขนานแท้ก็ถือกำเนิดขึ้นเป็นครั้งแรกในประเทศออสเตรเลีย เป็นไวรัสตัวแรก

ของโลกที่แพร่ระบาดบนวินโดวส์ 95 และรู้จักกันในชื่อว่า "Boza"

ไวรัส Boza จะแพร่ติดไฟล์นามสกุล .EXE ที่ออกแบบมาเฉพาะใช้งานบนวินโดวส์ 95 เท่านั้น โดยทุกครั้งที่มีการรันไฟล์ที่ติดไวรัสนี้ ไวรัส Boza ก็จะแพร่เข้าติดยังไฟล์นามสกุล .EXE อื่น ๆ อีก 1 - 3 ไฟล์ ที่อยู่ในไดเรคทอรีปัจจุบัน และจะไม่ทำการฝังตัวเองลงในหน่วยความจำ แต่จะค่อย ๆ แพร่กระจายไปยังไฟล์อื่น ๆ ในลักษณะเช่นนี้ต่อไปเรื่อย ๆ ตามลำดับอย่างช้า ๆ

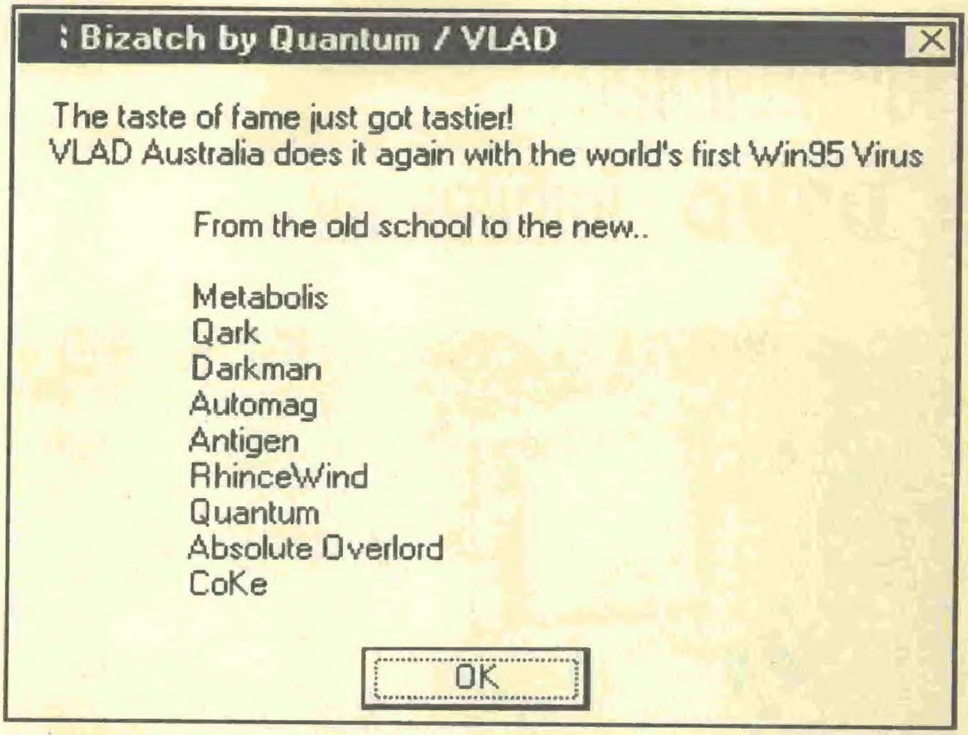
ไวรัส Boza นี้ถือว่าเป็นไวรัสที่มีการทำงานที่เรียบง่ายไม่ซับซ้อนอะไร และไม่ทำอันตรายใด ๆ ที่รุนแรงต่อระบบเลย จะมีก็แต่บักในตัวมันเองเท่านั้น ซึ่งอาจจะทำให้บางครั้งพบว่าขนาดของไฟล์นามสกุล .EXE ที่ติดไวรัสนี้เข้าไป มีขนาดใหญ่ขึ้นได้หลายเมกะไบต์ และไปมีผลทำให้พื้นที่ในดิสก์ลดน้อยลงอย่างรวดเร็ว

เมื่อไฟล์นามสกุล .EXE ในไดเรคทอรีปัจจุบันติดไวรัส Boza จนหมดครบทุกไฟล์แล้ว ไวรัสจะสุ่มแสดงข้อความในไดอะล็อก-บ็อกซ์ เพื่อบอกถึงชื่อผู้เขียน (ดูรูปที่ 1)

นอกจากนั้นยังพบว่า ภายในตัวไวรัสมีข้อความต่อไปนี้รวมอยู่ด้วย แต่จะไม่ปรากฏขึ้นบนจอภาพ

```
Please note : the name of this
virus is [Bizatch]
written by Quantum of VLAD.
```

ตัวโปรแกรมไวรัส Boza นี้ ถูกเขียนขึ้นให้เป็นไปตามมาตรฐานของ Win32 API ทั้งหมด เรียกได้ว่าเป็นไวรัส 32 บิตแบบเต็มตัว โดยจะทำการแก้ไขวินโดวส์ 95 executables ด้วยการเพิ่มเซกชันใหม่ลงไป และใช้ชื่อเฉพาะว่า ".vlad" ในส่วน header ของไฟล์ .EXE แบบ PE (PE หรือ Portable Executable คือไฟล์ EXE ฟอร์แมต 32 บิต บนวินโดวส์ 95) พร้อมทั้งระบุตำแหน่งของเซกชันนี้ไว้และจะทำการแก้ไขให้โปรแกรมชี้มาที่ตำแหน่งดังกล่าวซึ่งเป็นตัวไวรัสนั่นเอง



The taste of fame just got tastier!
VLAD Australia does it again with the world's first Win95 Virus

From the old school to the new..

Metabolis
Qark
Darkman
Automag
Antigen
RhinceWind
Quantum
Absolute Overlord
CoKe

รูปที่ 1

ไวรัส Boza จะใช้วิธีการง่าย ๆ ในการตรวจสอบตัวเอง ว่าครั้งหนึ่งเคยติดไปยังไฟล์นั้น ๆ แล้วหรือยัง โดยจะแก้ไขข้อมูลให้ที่ตำแหน่ง offset 4ch ซึ่งเป็นฟิลด์ที่ไม่ได้ถูกใช้งาน และอยู่ในส่วน header ของ PE จากเดิมที่เก็บเลข 0000 เป็นค่า F00DH แทน ค่านี้เองที่ไวรัส Boza จะนำมาใช้ในการตรวจสอบว่าตัวมันเองเคยติดไปที่ไฟล์นั้น ๆ มาก่อนแล้วหรือยัง

ตอนนี้บริษัทผู้ผลิตซอฟต์แวร์-ฮาร์ดแวร์ป้องกันไวรัสทุกค่ายก็กำลังหาวิธีตรวจจับไวรัส Boza นี้อยู่ เช่น Symantac และ McAfee รวมทั้ง R&D ของเราด้วย คาดว่าขณะนี้คงจะออกรุ่นใหม่ที่ป้องกันได้มาเกือบทุกค่ายแล้ว

หากเราจะลองนึกย้อนไปดูไวรัสบนดอสในสมัยแรก ๆ จะเห็นว่า เมื่อครั้งที่ไวรัสตัวแรกบนดอสถูกค้นพบในปี พ.ศ. 2532 นั้นก็ยังคงเป็นไวรัสที่มีเทคนิคง่าย ๆ ไม่ซับซ้อนอะไร เช่นเดียวกันกับไวรัส Boza ซึ่งเป็นไวรัสตัวแรกบนวินโดวส์ 95 และในปัจจุบันไวรัสบนดอสได้ถูกพัฒนาเทคนิคต่าง ๆ ขึ้นมากมายจนกระทั่งถึงขนาดเปลี่ยนร่างแปลงกายแบบ Polymorphic มีการหลบซ่อนตัวเองได้อย่างแนบเนียน แพร่ติดไฟล์ได้อย่างรวดเร็ว เมื่อเห็นดังนี้ก็อดที่จะคาดการณ์ไม่ได้ว่า ไวรัสบนวินโดวส์ 95 ก็คงจะถูกพัฒนาไปให้มีเทคนิควิธีการต่าง ๆ คล้าย ๆ กันกับที่ครั้งหนึ่งเคยเกิดขึ้นมาแล้วกับไวรัสบนดอสนั่นเอง!!!